

Lecture 14 - Security

Introduction

- An installation's data and programs are among its most valuable assets and must be protected
- At one time data was secure because no one knew how to access it
- As more people become computer literate and able to use simple tools unprotected data is becoming more accessible
- Data security is now more important than ever including the prevention of inadvertent destruction

Security is more than a click away!



Why security?

- Any system security must allow authorized users the access they need and prevent unauthorized access.
- Many companies' critical data is now on computer and is easily stolen if not protected
- z/OS Security Server provides a framework of services to protect data

Why use Security Tools

- Protect critical data from modification or inappropriate use
- Prevent accidental data corruption
- Manage protection and track unauthorized attempts

Security Concepts

- **Information Security has three basic concepts.**
 - Confidentiality (including authorization)
 - Integrity (including authentication)
 - Availability
- Each concept must be implemented in order to provide system security
- Depending on an organizations mission one of this three might hold higher importance than the other.

Security Concepts

Confidentiality

- You wish your information to remain just your information and protected from unauthorized access by someone else who might use it against you or to profit from it.
- It should remain protected and private to you or to a known and documented delegate.
- This is *confidentiality*.
- The most widespread form of confidentiality failure today leads to identity theft.
- Industrial espionage can also cause loss of confidentiality.

Threats to Confidentiality

Hackers

- There are as many different definitions of what hackers are as there are documents written about them. For our purpose a hacker is an individual who is skilled at bypassing controls and accessing data or information that he or she has not been given authorization to do so.
- Masqueraders
- Authorized users on the system that have obtained another persons credentials. Masquerading often occurs in companies with a low awareness of security concerns where users may share computers, and even passwords.
- We will also have to secure our computers from illegal access from within our company.

Unauthorized Users

- Within certain companies a certain “honor code” rule governs access to documentation and data. Users that do not observe the honor code and click on the resource (data or documents) gain access to the system.
- Unprotected Downloads
- Downloads of files from secure environments to non-secure environments or media compromises the security of the system.

Threats to Confidentiality

Malware

- Malware (virus and worms and other exploitation software) code seeks to either copy data from secure to insecure locations or to create an opening for its developers to access the protected resource.

Software hooks (Trapdoors)

- During the development phase software developers create “hooks” that allow them to bypass authentication processes and access the internal workings of the program. When the product development phase is over developers do not always remember the hooks and may leave them in place to be exploited by hackers.

Mis-delivered product or e-mail

- E-mail sent to a person with information about another customer or packages and other products delivered with account information sent to an unintended recipient.

Threats to Confidentiality

Exposure of sensitive information

- If we tracked a system process or message we may, at some time in its lifespan, find it residing unprotected in temporary buffers on a router, a gateway, or hosts. An experienced or even lucky hacker may take advantage.
- Wiretapping, hacking message delivery mechanisms, interception at source, destination or en-route are all examples of exposures.
- The tapes fell off the truck!

Confidentiality Models

- Flow Model

- lays out a scheme that relates objects (programs, files, computers that store information) with subjects (such as users, programs or systems) accessing the information.
- Information flows between equal classifications or from one classification level to a higher level never lower.

- Access Control Model

- In addition to the subjects and objects we have already detailed in the flow model, we have operations (the transaction taking place between the two).
- Sets of rules determine what operations may be performed by which subject and on which object giving the model much more control in assuring not only availability but also integrity

Roles and Separation of Duties

There are different functions that need to be conducted for the administration of data

The Security Administrator

- Performs the general definitions for all the required resources that need protecting, such as user IDs, datasets and general resources.

The Database Administrator

- Looks after the data contained within databases. Ensures availability to authorized users and maintains the backup and recovery functions.

•The Systems Programmer

- Ensures all the operating system parameters are in place to be sure that the system and the applications are performing correctly.

The Systems Operator

- Performs functions such as stopping and starting the computer, mounting tapes, responding to and interpreting and resolving error conditions.

Classification of Data

Data can be classified as a function of its importance. The methods available are:

Security levels

Where data can be classed with differing levels of importance by the allocation of a pre-determined number to rate the importance of the data. The higher the number allocated, the more secure. Level 1 might be general access but level 99 could be regarded as very important.

Classification names

Specific data elements can be classified to have higher or lower ranking for security than other data. Normal names are used and associated to differing level numbers for each name. Names like SECRET, SENSITIVE and UNCLASSIFIED are commonly used terms.

Labels

Also known as SECLABELs are a combination of security levels and categories. Labels are integral to providing a multi-secure environment.

Conditional & Temporal Access

Conditional access

- giving access to data when it is requested by a user and under certain conditions.
- The security administrator applies access to the resource so that the user can access only specific named data when certain conditions are met, such as executing a program from a particular library or from a particular terminal.

Temporal access

- A type of conditional access which allows users to access a system only during a predetermined time of the day or day of the week.
- Each user can be described for this attribute separately depending on his allowable and authorized function.

Discretionary and Mandatory Access Controls

- **There are two major access control policies for supporting confidentiality of information resources**
- **Discretionary access control**
 - Allows data owners to apply the level of access control through access control lists (ACLs) as they see fit or company security standard dictates.
 - The owners of the data use their discretion to allow different levels of access to data based on requirements of requester or their job role.
- **Mandatory access control**
 - Further enhances the discretionary access controls being used by including the use security labels. These controls allow greater security where systems are handling more sensitive data.
 - It is outside the discretion of the owners of the data and usually mandated by the security administrator or company security standards.

Authorization

- **The granting or denial of resource access to a user ID.**
- **Identification and Authorization work together to implement the “CIA” concepts of security**

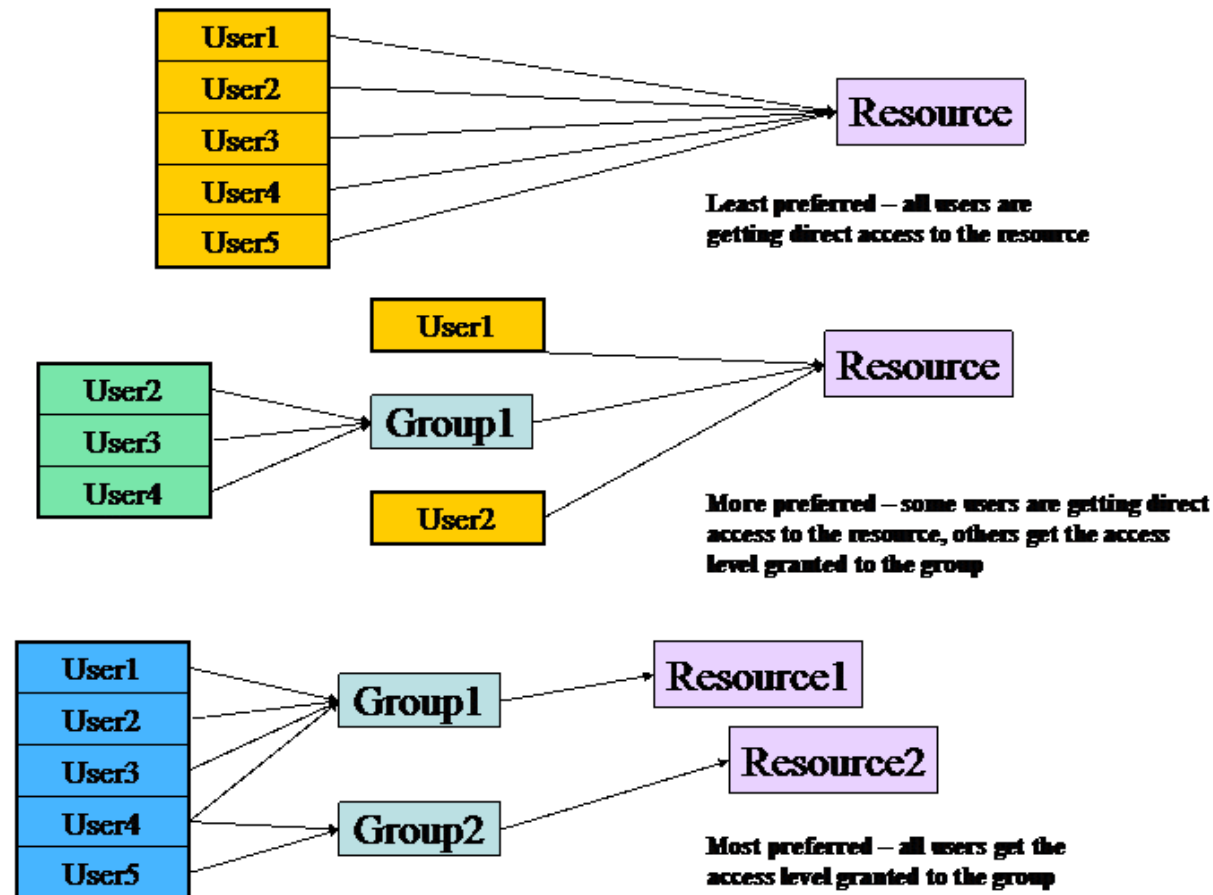
Authorization

- **Access Control Lists & Rules**

- Access control lists (ACLs) give you the ability to control the user accesses to resources.
- Each resource in the system needs to have a list of user IDs or groups associated with it that directly specifies who has what level of authority when they access it.
- These lists (or rules) are maintained by the security administrator at the higher level, but can be delegated to data owners who can manage their own resources.
- Depending on the environment, the resource owner can specify who can access the information, how it can be accessed, when it can be accessed, and under what conditions.

Authorization

Access Control Lists & Rules



Authorization

- **In a System z, the basic process flow to achieve authorization to a resource is:**
 - The user initiates an action which causes a request for access
 - The resource manager sends the request to the security product to determine if the user is allowed to have the access
 - The security product refers to the security database and does checking of resource for the user ID.
 - Based on the result of the checking, the security product returns a 'yes' or 'no' status back to the resource manager
 - The resource manager then allows the access or denies the request with an appropriate message for the user

Integrity

- Prevention of unauthorized modification of data
 - Intentional or accidental modification
- Integrity breaks down into:
 - Authenticity* - the information is from whomever we expect it to be and whatever we expect it to be.
 - Accountability* - the information has an owner or custodian who will stand by its contents.
 - Non-repudiation* - data transmission devices have built-in security features that includes a “signature” of the sender. The sender can’t repudiate or deny sending the data as long as his/her signature is included.

Security Concepts

Integrity

- The trustworthiness of your information is measured by your ability to detect when it has been modified, whether in storage, processing or transit.
- This is *integrity*.
- You must know with reasonable certainty that your information is accurate and will not mislead you or another recipient of it.
- The *proof* that your data has not been modified by unauthorized persons is the accountability that bank auditors seek the most.

Threats to Integrity

Salami-Slicing

- An attacker may insert code to siphon off fractions of pennies from each online transaction and redirect it into a customer account he creates. He may then have his program transfer the stolen money from the bank account into another bank's account where he can withdraw it.

Falsification

- An attacker's ability to alter a part of or all of a message, destroy a message to prevent delivery, or create unauthorized messages destroys our ability to distinguish between actual and falsified records.

Noise

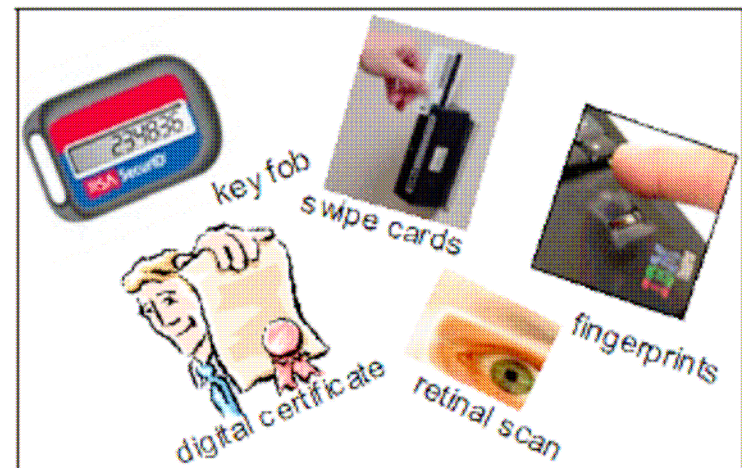
- Signal (electronic) traffic picks up electronic charges in the form of interference as it travels through media both from the medium it is traveling through, from natural sources such as lightning and static electricity as well as from man-made sources such as electric circuits and generators (motors).

Identification

- The ability to distinguish between users on the system protects data and resources from unwanted intrusion.
- Identification refers to a process of users identifying themselves to the computer and proving their identity so that the computer can allow them access.
- Every person who is required to perform any activity on the computer needs to be identified uniquely within that computer's security program.
- On System z computers, like most computers, your identity is confirmed through a user ID. Any access you require to data stored on this computer is applied by giving your user ID the permission to access it.

Authentication

- **Process by which the computer verifies identity.**
- **Authentication uses some combination of:**
 - What you know
 - What you have
 - What you are
- **Methods for performing authentication:**
 - user ID & Password
 - Swipe Card
 - Digital certificate
 - Key Fob
 - Biometrics



Security Concepts

Availability

- When we talk about access to your data, we are talking about *availability*.
- Anything that denies you the service of obtaining or saving your information is to be recognized, planned for, and avoided.
- This holds true whether you are the owner of the place of business or a customer of one.
- In the hardware arena, availability is synonymous with uptime, but when considered in the larger picture uptime isn't just a function of hardware, but of software stability and resilience to disaster or attack as well.
- Availability is about resilience, business continuity, and disaster recovery, ensuring backup information and systems are in place for recovery purposes.

Availability

- Resources that need to be accessed are accessible to authorized parties.
- If the confidentiality and integrity of the systems are assured, their availability for the purpose they are intended for is a direct consequence.

Threats to Availability

- Human Acts

- Unintentional

- Overwriting part or all of the data.
 - Compromising of Systems or Network Infrastructure by Organizational Staff

- Intentional

- Conventional Warfare
 - Informational Warfare
 - Denial of Service, Buffer overflow

Threats to Availability

- Non-Human
 - Fires, Floods, Earthquakes, and Storms
 - One of the most common events but one of the most over looked
 - Reasons for this:
 - Security plans rarely detail disaster recovery for IT systems.
 - Companies that do have a plan set the standards so high, they are hard to achieve.

Logging & Auditing

Logging

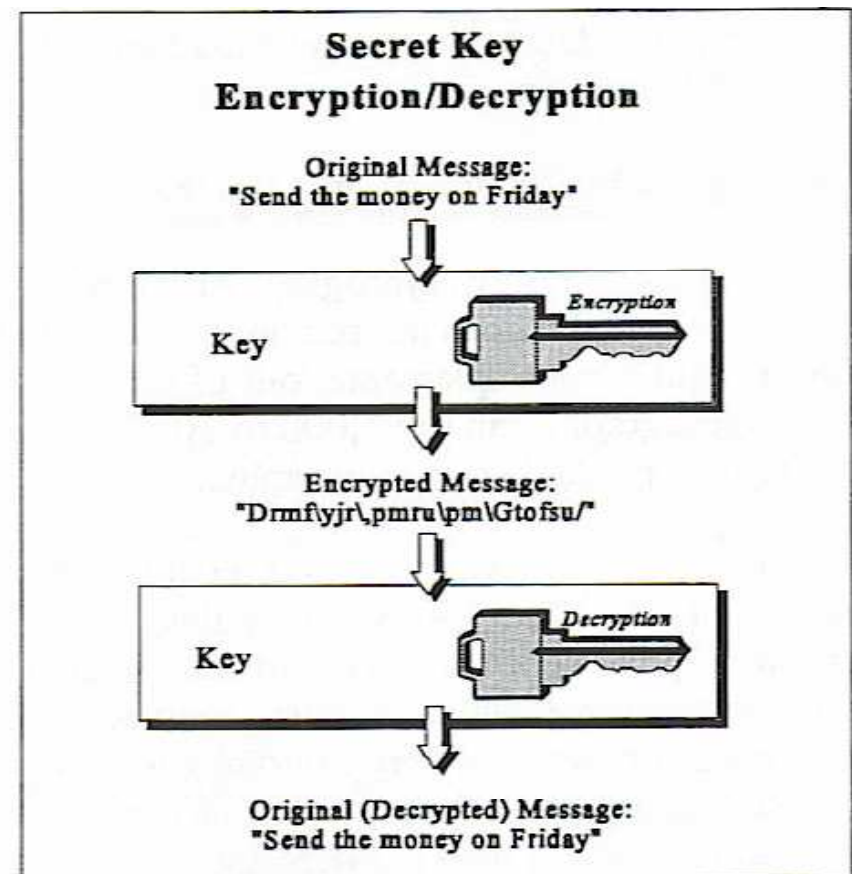
- Vital to problem determination, auditing, accountability, and system access reporting.
- The recording of data about specific events
- This recorded data is maintained in a data file, called a log, for later investigation.
- It should contain valid accesses as well as attempted compromises of system security controls.
- Some security products and tools are marketed that examine and present detailed reports that can be used to present facts on selective actions taken on System z.
- Auditing is the review of the logs on the mainframe. A systems auditor handles this and audits should be conducted on a set schedule along with random spot checks.**

Audits and change management

- Need to ensure everything is being done to minimize the risk.
- Audits produce records, and records can be compared to previous records to produce indicators of improvement. These are called metrics.
- Change happens, and changes must be controlled and recorded. Change records will be audited.
- Change management is a critical component of a security architecture and policy.

Encryption (Cryptography)

- Cryptography, the science behind the topic known as encryption, is the art of secret or disguised writing. It is thousands of years old and the written records of past great civilizations contain records of uses of such secret writing, including diplomatic and military communications.
- Encryption expands on this secret writing and deals with the methods involved in preparing coded text called ciphertext. This is data that is intended to be unintelligible to all except those who legitimately possess the means to reproduce it back to plain text.
- Conversion of the plaintext into ciphertext is called **enciphering** (or **encryption**) while the opposite conversion of ciphertext back to plaintext is called **deciphering** (or **decryption**).



Encryption & Security Concepts

Which security concept does encryption support?

Confidentiality (including authorization)

or

Integrity (including authentication)

or

Availability

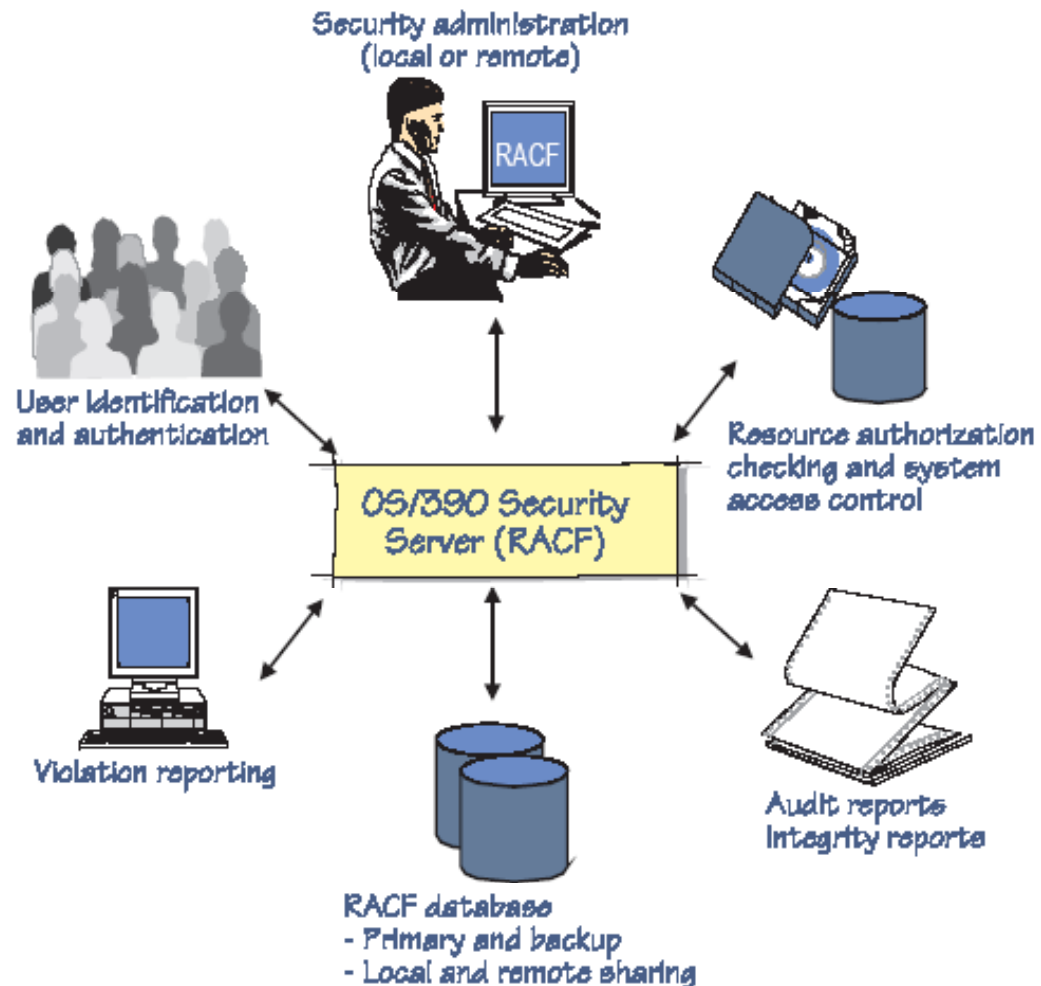
Security Tools - RACF

Mainframe Security Tools

- **RACF - Resource Access Control Facility - IBM mainframe security software that:**
 - Verifies user ID and password
 - Controls access to authorized files and resources.
- **ACF2 - Access Control Facility - A competing product from Computer Associates**
 - Concepts similar to RACF

What does RACF do?

- **Identify and authenticate** users
- **Authorize** users to access protected resources & data sets
- **Log and report** attempted unauthorized access
- **Security Admin** Control means of access to resources



RACF functions overview

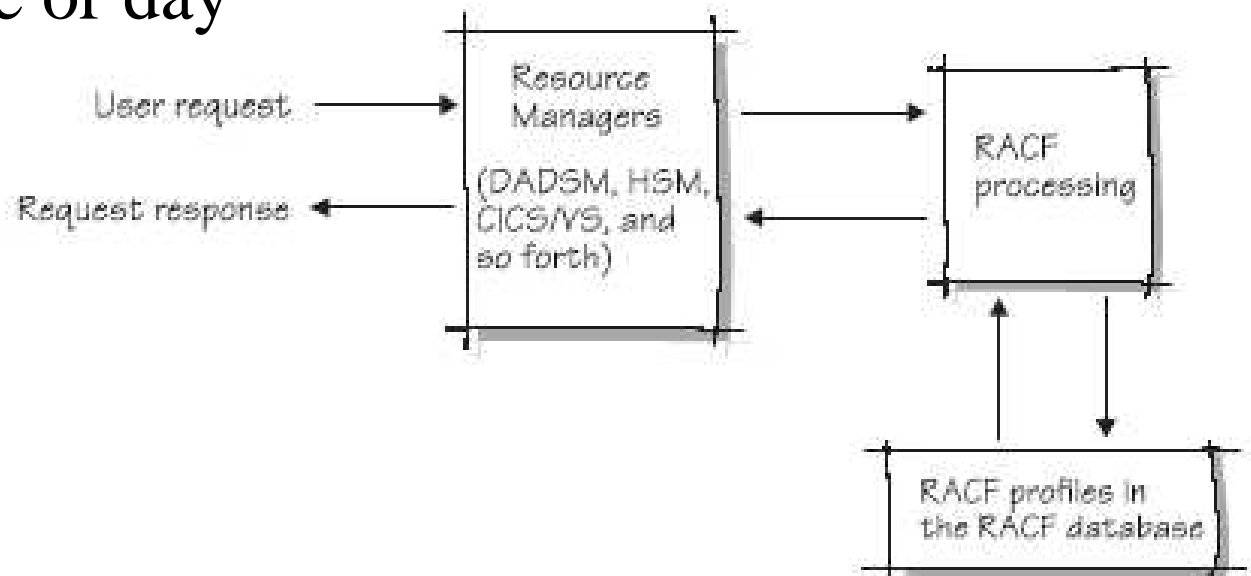


Identification and verification of users

- Identify **the person (or process) who is trying to gain access to the system**
- Authenticate **the user by verifying that the user is really that person**
- RACF uses a userid and system encrypted password to perform its user identification and verification
 - **The userid identified the person to the system**
 - **The password verifies the user's identity**
 - **Passwords should not be trivial and exits can be used to enforce policies.**

Authorization of users

- RACF controls the interaction between the user and the system resources
- RACF must authorize (based on profiles):
 - Which users may access which resources
 - How the user may access them (read, update), and by time or day



Logging and Reporting

- RACF maintains statistical information
 - date, time, number of times that a users accesses a resource
- RACF writes a security log when it detects:
 - Unauthorized attempts to enter the system
 - Access to resources
 - Authorized (or unauthorized) attempts to access RACF-protected resources**
 - This depends on the settings for the resource
 - For example `AUDIT(ALL(UPDATE))` will record all updates to a resource
 - Authorized (or unauthorized) attempts to enter RACF commands.

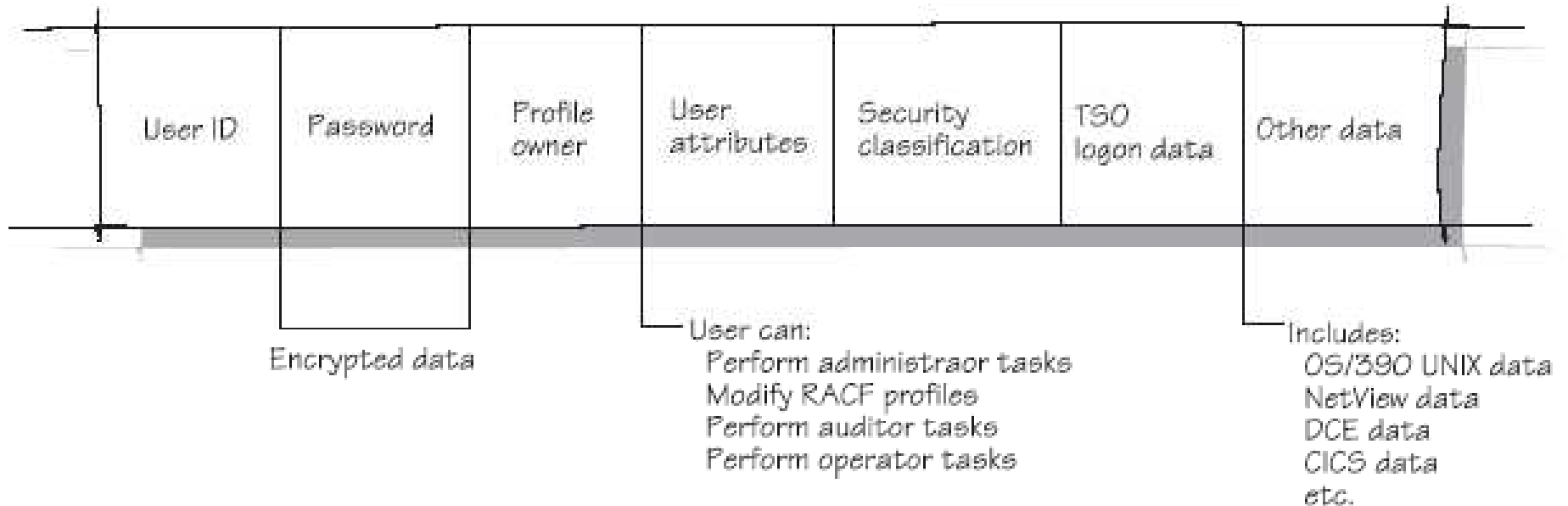
Security Administration

- Interpret the security policy to:
 - Determine which RACF functions to use
 - Identify the level of RACF protection
 - Identify which data to protect
 - Identify administrative structures and users

Profiles

RACF User Profiles

- RACF allows user profiles to be defined
- User profiles are stored in the RACF database



Data set Profiles: Protecting a dataset

- A data set profile is created and stored in the database
- It will give users or groups an access level
- A universal access level will also be set
- The profile can be specific or generic, with or without wild cards

General Resource Profiles:

Protecting general resources

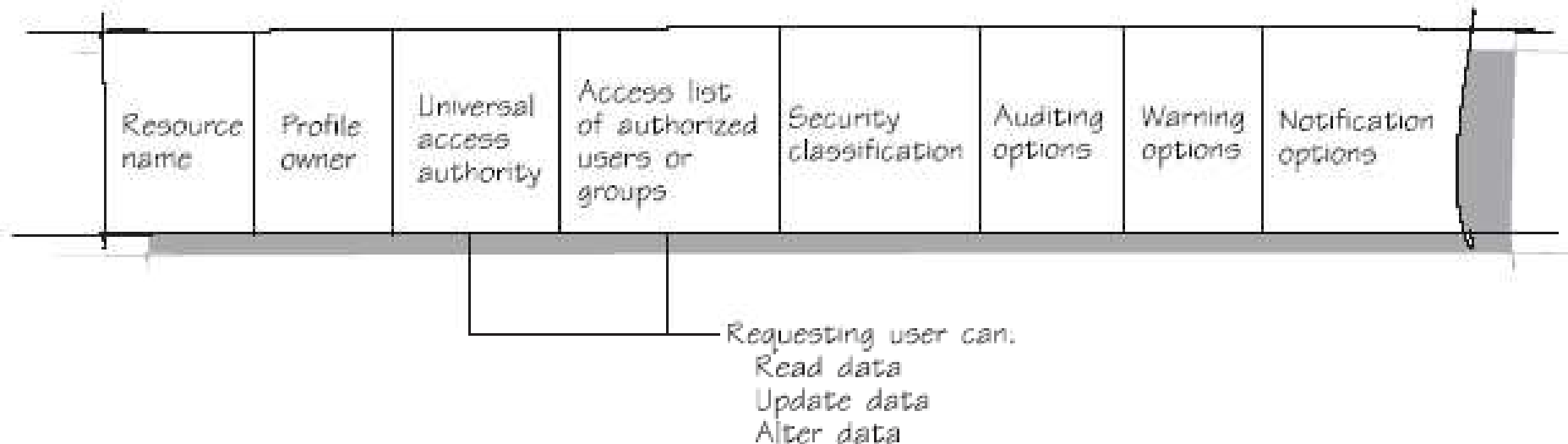
- Many system resources can be protected
 - DASD volumes
 - Tapes
 - CICS or IMS transactions
 - JES spool datasets
 - System commands
 - Application resources and many more
- RACF is flexible and more can be added

Protection Levels

- RACF works on a hierarchical structure
 - ALLOC allows data set creation and destruction
 - CONTROL allows VSAM repro
 - WRITE allows update of data
 - READ allows read of data
 - NONE no access
- A higher permission implies all those below

RACF Resource Profiles

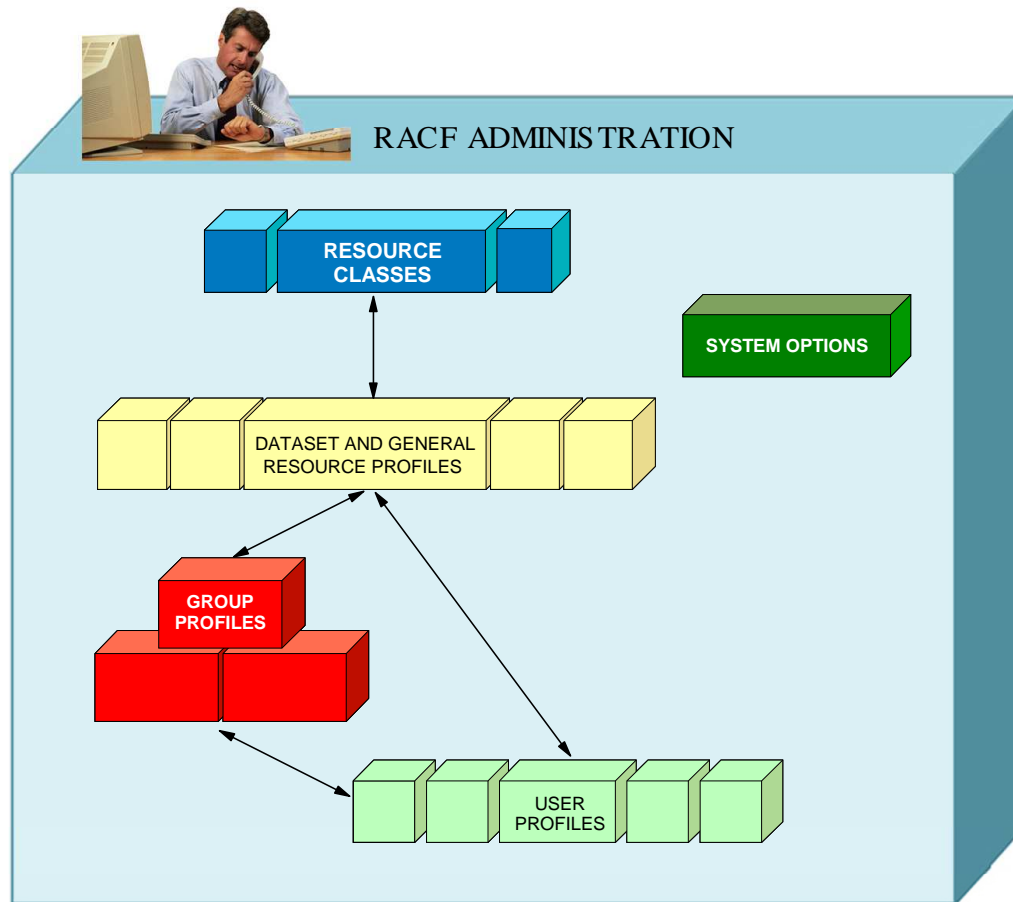
- Profiles are maintained in the RACF database
- Profiles are used to protect resources :
 - Data set profiles contain security info about DASD & tape data
 - General profiles contain security info on other resources
- Each RACF defined resource has a profile



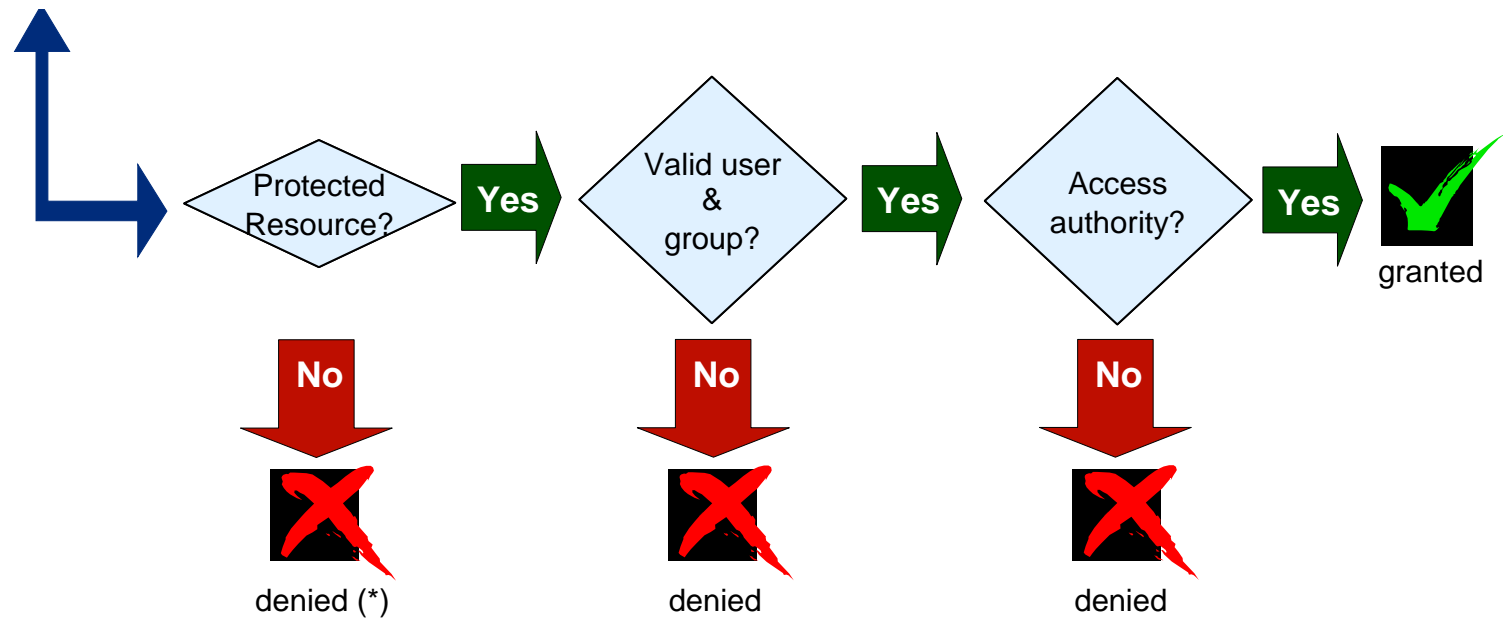
RACF Structure

- Userid
- Group
 - Every userid belongs to at least one group
 - Group structures are often used for access to resources
- Resource
- Resource classes
- Class descriptor table – used to customize

RACF structure overview

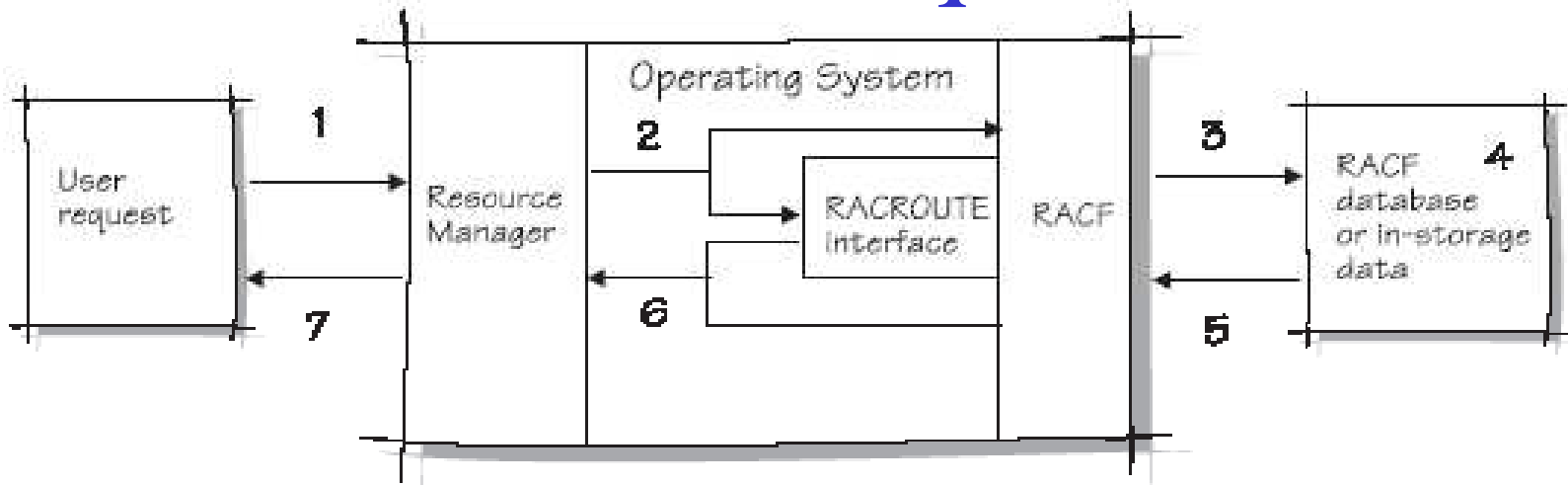


RACF profile checking



(*) if Protect All
option is in effect

RACF and it's relationship to a user's request



1. A user requests access to a resource using a resource manager (for example, TSO/E).
2. The resource manager issues a RACF request to see if the user can access the resource.
3. RACF refers to the RACF database or in-storage data and...
4. ...checks the appropriate resource profile.
5. Based on the information in the profile...
6. RACF passes the status of the request to the resource manager.
7. The resource manager grants (or denies) the request.

RACF & SYSPLEX Processing

Sysplex Security: RRSF - RACF Remote Sharing Facility

- If many systems share a RACF database there can be contention problems
- RACF will propagate commands throughout a sysplex
- RACF can use a coupling facility in a parallel sysplex to improve performance
- RRSF can be used to keep distributed RACF databases in line

Key Aspects / Benefits of a Security System

A security mechanism should:

How it benefits you:

<ul style="list-style-type: none">• Identify users who wish to access the secured system.	<ul style="list-style-type: none">• Lets you associate a unique identifier with each potential user of the system when the user enters the system.
<ul style="list-style-type: none">• Verify that the users are who they say they are.	<ul style="list-style-type: none">• Provides a further level of identification, such as a <i>password</i> or <i>PassTicket</i>, to verify that the user has the correct identifier upon accessing the system.
<ul style="list-style-type: none">• Allow only authorized users to access the protected resources.	<ul style="list-style-type: none">• Gives users the appropriate level of access authority for each protected resource.
<ul style="list-style-type: none">• Allow a convenient way to administer security.	<ul style="list-style-type: none">• Allows you to select the kind of security structure and administration to use at your installation.
<ul style="list-style-type: none">• Record accesses to protected resources.	<ul style="list-style-type: none">• Provides another level of accountability so you can see who is using what resources.• Allows you to define the records you require.
<ul style="list-style-type: none">• Document violations immediately or as a user-requested periodic report.	<ul style="list-style-type: none">• Lets you see the violations whenever you want in the format you choose.
<ul style="list-style-type: none">• Be usable by anyone whose data is being protected.	<ul style="list-style-type: none">• Is easy to define and easy to use. This helps to prevent circumventing the mechanism.
<ul style="list-style-type: none">• List the key protected resources and the level of protection that exists for each.	<ul style="list-style-type: none">• Allows you to see how each resource is protected.